Key Distribution using Quantum Cryptography

By

Ash Ghogale and Pulasti Choudhary

State of MD Information Technology
Security and Privacy Conference 2004

Classical Cryptography

- Some basic definitions
  - Cryptography – science of encrypting
  - Cryptanalysis – science of decrypting
  - Cryptology – discipline comprising of both
  - Plaintext - data to be encrypted
  - Ciphertext – encrypted message
  - Key - user selected data used to convert between plaintext and ciphertext

- Traditional techniques
  - Transposition
  - Substitution

Secret Key Encryption

- Symmetric: single key used to encrypt and decrypt
- Common techniques –
  - Block ciphers
  - Stream ciphers
- DES, triple-DES
- Key distribution problem
- Central key distribution server

Public Key Cryptosystem – Solution to Key Distribution Problem

- Asymmetric: a mailbox with two locks!
- Private key is always linked mathematically to the public key
- Clever mathematical solution – one way functions
- “Difficult” problems
- RSA – Based on Prime Number Factoring

PKC – Problems and Threats

- Technology advancements
  - “Confidence in the slowness of technological progress is all that the security of the current system rests upon”
- Mathematical advancements
  - Success depends on assumed-but-not-proven intrinsic difficulty of certain mathematical operations such as factoring large numbers (RSA)
  - Factoring Breakthroughs

Quantum Information And It’s Properties

- Qubit
  - Basic unit of Quantum information.
  - Could carry more than one states until measured!
- No-Cloning Theorem – *An unknown Quantum state can not be copied*
- Attempt to read information introduces disturbance
- Irreversibility of measurement

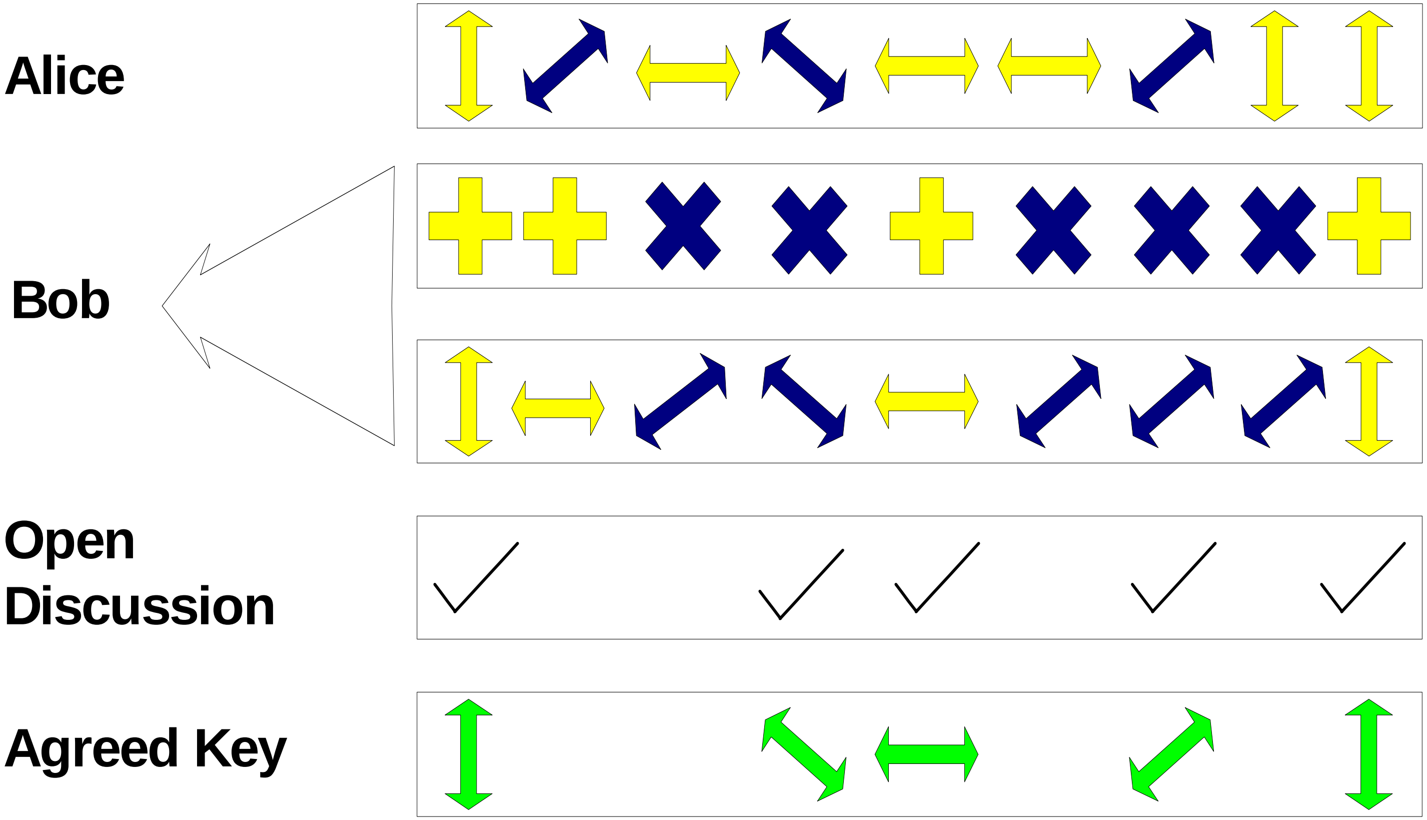
Quantum Key Distribution - An Alternative to PKC

- BB84 Protocol
  - Tolerable error rate – sacrifice some communication to test for eavesdropping
  - Key Storage Problem - EPR Scheme based on the entanglement
  - Efficiency

- Other schemes
  - Multi-user network protocol
  - No public discussion protocol

BB84

Bennett-Brassard 1984



Alice

Bob

Open Discussion

Agreed Key

Back

Limitations of Quantum Key Distribution

- Jamming the channel
- Man in the middle
- Single photon transmission
- Noise – not distinguishable from eavesdropping
- Transmission Mechanism and Frequency

Quantum Cryptanalysis

- Quantum Computing can efficiently solve factoring and elliptic curves problem
- Shor’s (1994) “hidden linear form” algorithm to cryptanalysis
- Grover’s algorithm for exhaustive key search against DES
- Conventional Crypto systems will be unsafe!

Feasibility of Quantum Cryptography

- Increase in Security

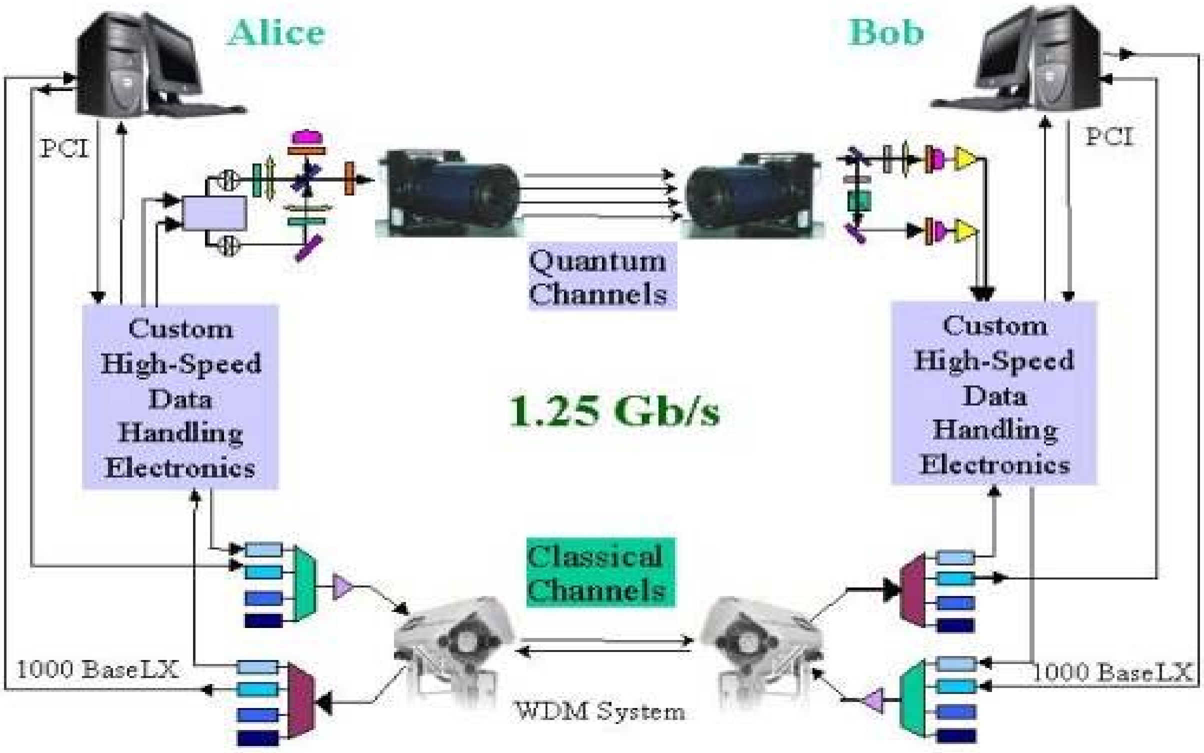
  => Increase in Cost

  => Decrease in Practical Interest

- Progress in technology more predictable than progress in mathematics

- “Retrospective” Attack is not possible

Example QKD Network



Reference : NIST

QISET Meeting April 29, 2004

Latest Developments

- First QC Financial transaction performed by Bank of Austria on behalf of City of Vienna performed on April 21,2004
- NIST Demo May 2004 – Sets Speed Record

Application for Industry and Users

- Implementation Drivers
  - Mathematical breakdown of PKC
  - Technological advancement in quantum computing
  - Need to keep some secrets for ever

- Someone could be storing all the transactions to be deciphered at later date

- Target Implementations
  - Govt.Departments, banks and financial institutes looking to archive information over ultra secure links are expected to be the first ones to use this technology
  - It is also expected that this technology will be used to reinforce the security of E-Voting applications through tamper and eavesdropping detection via Quantum channel connecting Central Govt.servers with local county servers[1]

Sources:

[1] Product Vendor (WISeKey Press Release)

Defining and designing Security Policies and Procedures

- Standards have to keep pace with technological advances.
- FIPS impacts
  - NIST News release on FIPS 46-3
  - FIPS 171
- Security Policy – Where will it be impacted
- Elimination of Key maintenance overhead
- Focus in the policies and procedures will shift from Secret Key Management Procedures more towards actual Data transmissions and management
- With properly implemented QC, attacking the key becomes virtually impossible despite increased computing power

Implications on Executive Decision Making

- Rewards
  - Business Processes will become much more efficient, faster, transparent
  - Tamper Proof guarantee
  - Periodic Security Scans and Intrusion Detection runs could be eliminated
  - Variety of funding opportunities available for partnering in QC research
- Risks
  - Cost
  - Emerging Technology

Preparing for the Future

- Design future Architectures that are able to support an Integrated Mix of Foundation and Emerging technologies
- Look for partnership opportunities in QC
  - Test Beds for Quantum Cryptography Policy and Procedures (NIST ,US Govt, Universities)
  - Policies and Procedures are business specific hence Govt. and Universities are actively looking forward to Agency and Pvt. Sector participation in these projects
- Keeping abreast of latest technological advancements helps us to start thinking about their application and integration in current Business Processes

References

- qubit.nist.gov
- www.itl.nist.gov
- www.governmententerprise.com/showArticle.jhtml?articleID=21400688
- www.qubit.org
- www.gap-optique.unige.ch/Publications/Pdf/QC.pdf
- www.csa.com/hottopics/crypt/overview.html
- www.ecst.csuchico.edu/~atman/Crypto/quantum/quantum-index.html
- www.rsa.com
- www.magiqtech.com
- www.wisekey.com